Palo Alto Networks VM-Series FIPS 140-2 Non-Proprietary Security Policy

Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054

www.paloaltonetworks.com

Revision Date: October 1, 2018

Change Record

Date	Author	Description of Change
11/15/2017	Amir Shahhosseini	Initial authoring for PAN-OS 8.0
2/14/2018	Amir Shahhosseini	Minor updates
6/14/2018	Amir Shahhosseini	Added software version 8.0.6 and 8.0.9
6/21/2018	Amir Shahhosseini	Fixed typo
10/1/2018	Amir Shahhosseini	Added software version 8.0.12 and 8.0.13

Contents

Tables

Figures

Module Overview

The Palo Alto Networks VM Series Firewall is available in multiple capacity options (e.g., VM-50, VM-100, VM-200, VM-300, VM-500 and VM-700; note that these are sets of configuration options rather than actual module variants). All models can be deployed as guest virtual machines on VMware ESXi, Hyper-V 2012 R2 and Linux server that is running the KVM (Kernel-based Virtual Machine) using a common base image distributed in a compatible hypervisor format.

Table 1 - Module Files

Operating Environment	PA-VM Release Version
VMware ESXi v5.5	8.0.3, 8.0.6, 8.0.9, 8.0.12, or 8.0.13
KVM on CentOS 7.2	8.0.3, 8.0.6, 8.0.9, 8.0.12, or 8.0.13
Microsoft Hyper-V 2012R2	8.0.3, 8.0.6, 8.0.9, 8.0.12, or 8.0.13
Amazon AWS*	8.0.3, 8.0.6, 8.0.9, 8.0.12, or 8.0.13
Microsoft Azure*	8.0.3, 8.0.6, 8.0.9, 8.0.12, or 8.0.13

Please see Section 7 of this document for this listing of tested configurations of these module files.

The Palo Alto Networks VM Series Firewall is a software cryptographic module and requires an underlying general purpose computer (GPC) environment. The module is comprised of a GPC (multi-chip standalone embodiment) and the Logical Cryptographic Module (LCM) boundary. The LCM boundary includes all of the logical software components of the module. The physical cryptographic module (PCM) boundary is defined by the enclosure around the host GPC on which it runs.

Figure 1 depicts the logical diagram for the LCM boundary and illustrates the hardware components of a GPC.

*Note: These operational environments are Vendor Affirmed. See Section 8 in this Security Policy for operator porting rules.

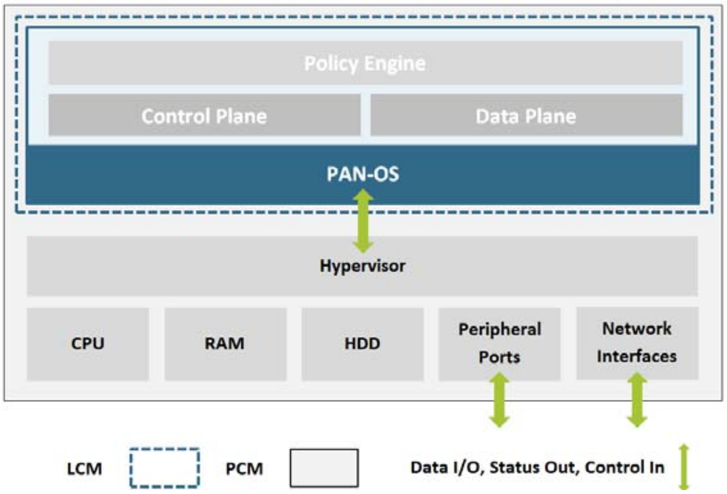

Figure 1 – Cryptographic Boundary

1 Security Level

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

Table 2 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	3
Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A

2 Modes of Operation

2.1 FIPS Approved Mode of Operation

The modules support both a CC mode (FIPS mode) and a non-CC mode. The following procedure will put the modules into the FIPS-approved mode of operation:

- During initial boot up, break the boot sequence via the console port connection (by entering "maint") to access the main menu.
- Select "Continue."
- Select the "Set FIPS-CC Mode" option to enter CC mode.
- Select "Enable FIPS-CC Mode".
- When prompted, select "Reboot" and the module will re-initialize and continue into CC mode (FIPS mode).
- The module will reboot.
- In FIPS-CC mode, the console port is available only as a status output port.
- If using RADIUS or TACACS+, configure the service route via an IPSec tunnel. Otherwise, skip this step.

The module will automatically indicate the FIPS Approved mode of operation in the following manner:

- Status output interface will indicate "**** FIPS-CC MODE ENABLED ****" via the CLI session.
- Status output interface will indicate "FIPS-CC mode enabled successfully" via the console port.
- The module will display "FIPS-CC" at all times in the status bar at the bottom of the web interface.

Should one or more power-up self-tests fail, the FIPS Approved mode of operation will not be achieved. Feedback will consist of:

- The module will reboot and enter a state in which the reason for the reboot can be determined.
- The module will output "FIPS-CC failure"
- To determine which self-test caused the system to reboot into the error state, connect the console cable and follow the on-screen instructions to view the self-test output.

2.2 *Approved and Allowed Algorithms*

The cryptographic modules support the following FIPS Approved algorithms.

Table 3 - FIPS Approved Algorithms Used in Current Module

FIPS Approved Algorithm	CAVP Cert. #
AES [FIPS 197, SP800-38A]: - ECB, CBC, CTR modes; Encrypt/Decrypt; 128, 192 and 256-bit - CFB mode; Encrypt/Decrypt; 128 bit Note: AES-OFB (128, 192, 256 bit) and AES-CFB (192, 256 bit) were also tested but are not available for use	4526
AES-CCM [SP800-38C]: Encrypt and Decrypt, 128-bit	4526
AES-GCM [SP800-38D]: Encrypt and Decrypt, 128 and 256-bit Note: GCM IV handling is compliant with FIPS IG A.5 and SP800-38D.*	4526
CKG (SP800-133) Key Generation Vendor Affirmed -Asymmetric per Section 6 -Symmetric per Section 7	N/A
CVL: Elliptic Curve Diffie-Hellman Exchange [SP800-56A] - ECC CDH primitive (§5.7.1.2) - KAS-ECC all except KDF	CVL 1203
CVL: Diffie-Hellman Exchange [SP800-56A] - KAS-FFC all except KDF	CVL 1203
CVL: KDF, Application Specific [SP800-135] - TLS 1.0/1.1/1.2 KDF - SNMPv3 KDF - SSHv2 KDF - IKE v1/v2 KDF	CVL 1204
CVL: RSA [SP800-56B] - RSADP	CVL 1205
DRBG [SP800-90A]: CTR DRBG with AES-256	1486
DSA [FIPS 186-4]: Key Generation (as prerequisite to CVL #1203)	1205
ECDSA [FIPS 186-4] - Key Pair Generation P-256, P-384 and P-521 - Signature Generation P-256, P-384 and P-521; with all SHA-2 sizes*	1101

FIPS Approved Algorithm	CAVP Cert. #
- Signature Verification P-256, P-384 and P-521; with SHA-1 and all SHA-2 sizes* *Does not include the "short SHA-512" sizes SHA-512/224 or SHA-512/256	
HMAC [FIPS 198] - HMAC-SHA-1 with λ=96, 160 - HMAC-SHA-256 with λ=256 - HMAC-SHA-384 with λ=384 - HMAC-SHA-512 with λ=512	2986
KAS: SP 800-56A Rev.2 Elliptic Curve Diffie-Hellman Exchange (CVL Certs. #1203 and #1204, vendor affirmed; key agreement; key establishment methodology provides between 128 and 256 bits of encryption strength)	N/A
KAS: SP 800-56A Rev.2 Diffie-Hellman Exchange (CVL Certs. #1203 and #1204, vendor affirmed; key agreement; key establishment methodology provides 112 bits of encryption strength)	N/A
KTS [SP800-38F §3.1]: Option 1: AES-CBC plus HMAC Option 2: AES-GCM (Key wrapping; key establishment methodology provides between 128 bit and 256 bits of encryption strength)	AES 4526 HMAC 2986
FIPS 186-4 RSA [FIPS 186-4]: - Key Generation: 2048 and 3072-bit - Signature Generation: 2048 and 3072-bit - Signature Verification: 1024, 2048 and 3072-bit - Hashes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 - Padding: X9.31, PKCS 1.5, PSS (Refer to RSA Cert. #2463 for the exact keysize/padding/hash combinations in use.)	2463
SHA-1 and SHA-2 [FIPS 180-4]: - Hashes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 - Usage: Digital Signature Generation & Verification, Non-Digital Signature Applications (e.g., component of DRBG and HMAC)	3707

* The module is compliant to IG A.5: GCM is used in the context of TLS, IPsec/IKEv2, SSH, and IPsec/IKEv1:

- For TLS, The GCM implementation meets Option 1 of IG A.5: it is used in a manner compliant with SP 800-52 and in accordance with Section 4 of RFC 5288 for TLS key establishment. (From this RFC, the GCM cipher suites in use are TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, and TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384.) During operational testing, the module was tested against an independent version of TLS and found to behave correctly.

- For IPsec/IKEv2, The GCM implementation meets Option 1 of IG A.5: it is used in a manner compliant with RFCs 4106 and 7296 (RFC 5282 is not applicable, as the module does not use GCM within IKEv2 itself). During operational testing, the module was tested against an independent version of IPsec with IKEv2 and found to behave correctly.
- For SSH, the module meets Option 4 of IG A.5. The fixed field is 32 bits in length and is derived using the SSH KDF; this ensures the fixed field is unique for any given GCM session. The invocation field is 64 bits in length and is incremented for each invocation of GCM; this prevents the IV from repeating until the entire invocation field space of 2^{64} is exhausted. (It would take hundreds of years for this to occur.)
- For IPsec/IKEv1, the module meets Option 4 of IG A.5. The behavior is the same as the above description for SSH, except the fixed field is derived using the IKEv1 KDF instead of the SSH KDF.

In all of the above cases, the nonce_explicit is always generated deterministically.

The cryptographic modules support the following non-FIPS Approved algorithms that are allowed for use in CC (FIPS) mode.

Table 4 - FIPS Allowed Algorithms Used in Current Module

FIPS Allowed Algorithms
Diffie-Hellman, non-compliant to SP800-56A [safe primes: L=2048, N=2047] (key agreement; key establishment methodology provides 112 bits of encryption strength)
RSA unwrap, non-compliant to SP800-56B (key wrapping, key establishment methodology provides 112 or 128 bits of encryption strength)
MD5 (within TLS)
NDRNG (used to seed SP800-90A DRBG) This provides a minimum of 128 bits of entropy.

Table 5 - Supported Protocols in FIPS Approved Mode

Supported Protocols*
TLSv1.0, 1.1 and v1.2
SSHv2
IPSec, IKEv1 and V2
SNMPv3

*Note: These protocols have not been tested or reviewed by the CMVP or the CAVP.

2.3 Non-Approved, Non-Allowed Algorithms

The cryptographic modules support the following non-Approved algorithms in the non-Approved mode of operation. No security claim is made in the current modules for any of the following non-Approved algorithms.

Table 6 - Non-Approved, Non-Allowed Algorithms Used in Current Module

Non-Approved Algorithms in Non-FIPS mode
Hashing: RIPEMD, MD5
Encrypt/Decrypt: Camellia, SEED, Triple-DES (non-compliant), Blowfish, CAST, RC4, DES
Message Authentication: UMAC, HMAC-MD5, HMAC-RIPEMD
Digital Signatures (non-Approved strengths): RSA Key Generation: 512, 1024 RSA signature generation: Modulus bit length less than 2048 or greater than 3072 bits; up to 16384 bits RSA signature verification: Modulus bit length less than 1024 or greater than 3072 bits; up to 16384 bits ECDSA: B, K, P curves not equal to P-256, P-384 or P-521 DSA: 768 to 4096 bits
Key Exchange (non-Approved strengths): Elliptic Curve Diffie-Hellman: B, K, P curves not equal to P-256, P-384 or P-521 Diffie-Hellman: 768, 1024 and 1536 bit modulus RSA: Less than 2048 bit modulus

3 Ports and Interfaces

The module is a software only module that operates on a general purpose computing (GPC) platform. The physical ports and logical interfaces are consistent with a GPC operating environment. The module supports the following FIPS 140-2 logical interfaces:

Table 7 - Module Ports and Interfaces

Type	FIPS 140-2 Designation	GPC Peripheral Ports and Network Interfaces
Management/ Ethernet	Data Input, Data Output, Control Input, Status Output	Ethernet
Console	Status Output	Ethernet, GPC I/O
Power	Power	Power

The module’s physical and electrical characteristics, manual controls, and physical indicators are provided by the host GPC; the hypervisors provide virtualized ports and interfaces which map to the GPCs’ physical ports and interfaces (i.e., network interfaces and GPC inputs/outputs).

4 Identification and Authentication Policy

4.1 Assumption of Roles

The modules support four distinct operator roles, User and Cryptographic Officer (CO), Remote Access VPN, and Site-to-site VPN. The cryptographic modules enforce the separation of roles using unique authentication credentials associated with operator accounts. The modules support concurrent operators.

The modules do not provide a maintenance role or bypass capability.

Table 8 - Roles and Required Identification and Authentication

Role	Description	Authentication Type	Authentication Data
CO	This role has access to all configurations, show status and update services offered by the module. Within the PAN-OS software, this role maps to the "Superuser" administrator role.	Identity-based operator authentication	Username/password and/or public-key/certificate based authentication
User	This role has limited access to services offered by the modules. This role does not have access to modify or view the passwords associated with other administrator accounts The User may not view or alter CSPs of any type stored on the module. The User may change their own password. Within the PAN-OS software, this role maps to the "Superuser (read-only)" administrator role (also referred to as "Superreader").	Identity-based operator authentication	Username/password and/or public-key/certificate based authentication
Remote Access VPN (RA VPN)	Remote user accessing the network via VPN.	Identity-based operator authentication	Username/password and/or certificate based authentication

Role	Description	Authentication Type	Authentication Data
Site-to-site VPN (S-S VPN)	Remote VPN device establishing a VPN session to facilitate access to the network.	Identity-based operator authentication	IKE/IPSec Pre-shared keys - Identification with the IP Address and authentication with the Pre-Shared Key or certificate based authentication

Table 9 - Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username and Password	Minimum length is 6 characters (95 possible characters). The probability that a random attempt will succeed or a false acceptance will occur is 1/(95^6) which is less than 1/1,000,000. The probability of successfully authenticating to the module within one minute is 10/(95^6), which is less than 1/100,000. The firewall's configuration supports at most ten attempts to authenticate in a one-minute period.
Public-Key/Certificate based authentication	The security modules support public-key based authentication using RSA 2048 and certificate-based authentication using RSA 2048, RSA 3072, ECDSA P-256, P-384, or P-521. For RSA, the minimum equivalent strength supported is 112 bits. The probability that a random attempt will succeed is 1/(2^{112}) which is less than 1/1,000,000. The probability of successfully authenticating to the module within a one minute period is 3,600,000/(2^{112}), which is less than 1/100,000. The firewall supports at most 60,000 new sessions per second to authenticate in a one-minute period. For ECDSA, the minimum equivalent strength supported is 128 bits. The probability that a random attempt will succeed is 1/(2^{128}) which is less than 1/1,000,000. The probability of successfully authenticating to the module within a one minute period is 3,600,000/(2^{128}), which is less than 1/100,000. The firewall supports at most 60,000 new sessions per second to authenticate in a one-minute period.

Authentication Mechanism	Strength of Mechanism
IKE/IPSec pre-shared keys	The 160 bit key length supports 2^{160} different combinations. The probability of successfully authenticating to the module is $1/(2^{160})$, which is less than 1/1,000,000. The number of authentication attempts is limited by the number of new connections per second supported (120,000) on the fastest platform of the Palo Alto Networks firewalls. The probability of successfully authenticating to the module within a one minute period is $7,200,000/(2^{160})$, which is less than 1/100,000.

5 Access Control Policy

5.1 Roles and Services

The Approved and non-Approved mode of operation provide identical services. While in the Approved mode of operation all CO and User services are accessed via SSH or TLS sessions. Approved and allowed algorithms, relevant CSPs and public keys related to these protocols are accessed to support the following services. CSP access by services is further described in the following tables.

The services listed below are also available in the non-Approved mode. In the Non-Approved mode SSH, TLS and VPN processes will use non-Approved Algorithms and Approved algorithms with non-approved strength.

Table 10 - Authenticated Service Descriptions

Service	Description
Security Configuration Management	Configuring and managing cryptographic parameters and setting/modifying security policy, including creating User accounts and additional CO accounts.
Other Configuration	Networking parameter configuration, logging configuration, and other non-security relevant configuration.
View Other Configuration	Read-only of non-security relevant configuration (see above).
Show Status	View status via the web interface, command line interface or VPN session
VPN	Provide network access for remote users or site-to-site connections.

Software Update	Provides a method to update the software on the firewall.

Note: Additional information on the configuration options the module provides can be found at https://www.paloaltonetworks.com/documentation.html

Table 11 - Authenticated Service Access

Service	Crypto Officer	User	RA VPN	S-S VPN
Security Configuration Management	Y	Y	N	N
Other Configuration	Y	N	N	N
View Other Configuration	Y	Y	N	N
Show Status	Y	Y	Y	Y
VPN	N	N	Y	Y
Software Update	Y	N	N	N

5.2 Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

Table 12 - Unauthenticated Services

Service	Description
Zeroize	The device will overwrite all CSPs.
Self-Tests	Run power up self-tests on demand by power cycling the module.
Show Status	View status of the module via hypervisor. (e.g. power status)

The zeroization procedure is invoked when the operator exits CC (FIPS) mode. The operator must be in control of the module during the entire procedure to ensure that it has successfully completed. During the zeroization procedure, no other services are available.

5.3 Definition of Critical Security Parameters (CSPs)

The modules contain the following CSPs:

Table 13 - Private Keys and CSPs

CSP #	Key Name	Type	Description
1	RSA Private Keys	RSA	RSA Private key for generation of signatures, authentication and key establishment (RSA 2048 or 3072 bits)
2	ECDSA Private Keys	ECDSA	ECDSA Private key for generation of signatures and authentication (P-256, P-384 or P-521)
3	TLS PreMaster Secret	TLS Secret	Secret value used to derive the TLS session keys
4	TLS DHE Private Components	DH, ECDH	Diffie-Hellman private FFC or EC component (DHE 2048, ECDHE P-256, P-384, P-521)
5	TLS HMAC Keys	HMAC	TLS integrity and authentication session keys (SHA1, SHA256 and SHA384)
6	TLS Encryption Keys	AES	TLS encryption session keys (128 and 256 CBC or GCM)
7	SSH Session Authentication Keys	HMAC	Authentication keys used in all SSH connections to the security module's command line interface. (SHA1)
8	SSH Session Encryption Keys	AES	Used in all SSH connections to the security module's command line interface. (128, 192 and 256 CBC or CTR)
9	SSH DH Private Components	DH	Diffie Hellman private component used in key establishment (DHE 2048, ECDHE P-256, P-384, P-521).
10	S-S VPN IPSec/IKE authentication Keys	HMAC	Used to authenticate the peer in an IKE/IPSec tunnel connection. (SHA1, SHA256, SHA384 or SHA 512)
11	S-S VPN IPSec/IKE session Keys	AES	Used to encrypt IKE/IPSec data. These are AES (128, 192, or 256 CBC) IKE keys and (128, 192 or 256 CBC, 128 CCM, 128 or 256 GCM) IPSec keys

CSP #	Key Name	Type	Description
12	S-S VPN IPSec/IKE Diffie Hellman Private Components	DH, ECDH	Diffie Hellman private component used in key establishment (DHE 2048, ECDHE P-256, P-384)
13	S-S VPN IPSec pre-shared Keys	Part of HMAC	Manually distributed by an administrator in the CO role. Used in authentication.
14	RA VPN IPSec session Keys	AES	Used to encrypt remote access sessions utilizing IPSec. (128 CBC)
15	RA VPN IPSec authentication HMAC	HMAC	Used in authentication of remote access IPSec data. (SHA-1)
16	Software Content Encryption Key	AES	Used to decrypt software and content. (AES-CBC 256)
17	CO, User, RA VPN Password	Password	Used to authenticate operator
18	DRBG Seed /State	DRBG	Used by DRBG. Includes the V and the Key.
19	SNMPv3 Secrets	SNMPv3 Secrets	SNMPv3 Authentication Secret and Privacy Secret
20	SNMPv3 Keys	SNMPv3 Keys	AES CFB Privacy key and HMAC-SHA-1 Authentication keys

Note: Transient CSPs are zeroized by an overwrite with a pseudo random pattern followed by read-verify. Intermediate plaintext key material (CSP) is zeroized when it is copied from one to another memory location. All keys (CSPs) are zeroized when they expire. Session keys (CSPs) are zeroized as soon as the associated session has ended/timed out/ or been closed. Private keys (CSPs) are zeroized when their corresponding public keys (certificates) expire.

5.4 *Definition of Public Keys*

The modules contain the following public keys:

Table 14 - Public Keys

	Key Name	Description
A	CA Certificates	Used to extend trust for certificates (RSA 1024, 2048 or 3072 bits and ECDSA P-256, P-384 or P-521)
B	ECDSA Public Keys / Certificates	ECDSA Public keys managed as certificates for the verification of signatures, establishment of TLS, operator authentication and peer authentication. (ECDSA P-256, P-384, or P-521)
C	RSA Public Keys / Certificates	RSA Public keys managed as certificates for the verification of signatures, establishment of TLS, operator authentication and peer authentication. (RSA 2048 or 3072 bits)
D	TLS DH public components	Used in key agreement (DHE 2048, ECDHE P-256, P-384 and P-521)
E	SSH DH public components	Used in key agreement (DHE 2048, ECDHE P-256, P-384, P-521)
F	SSH Host public key	SSH Host Public Key (RSA 2048, ECDSA P-256, P-384, or P-521) (The matching private key is among the RSA Private Keys or ECDSA Private Keys, in Table 13.)
G	S-S VPN - IPSec/IKE Diffie Hellman public component	Used in key agreement (DHE 2048, ECDHE P-256, P-384)
H	Public Key for software content load test	Used to authenticate software and content to be installed on the firewall (RSA 2048 with SHA-256)
I	Software Authentication Key	RSA key used to authenticate software (2048 bit RSA with SHA-256)
J	Software Integrity verification key	Public key used to validate firmware integrity at power-up (ECDSA P-256)

5.5 Definition of CSPs Modes of Access

Table 15 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- **R** = Read: The module reads the CSP. The read access is typically performed before the module uses the CSP.
- **W** = Write: The module writes the CSP. The write access is typically performed after a CSP is imported into the module, or the module generates a CSP, or the module overwrites an existing CSP.
- **Z** = Zeroize: The module zeroizes the CSP.

Table 15 - CSP Access Rights within Roles & Services

Role	Authorized Service	Mode	Cryptographic Key or CSP
CO	Security Configuration Management	RW	1, 2, 3, 4, 5, 6, 7, 8, 9, 16, 17, 18, 19, 20, A, B, C, D, E, F, G, I
CO	Other Configuration	RW	1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, G
User, CO	View Other Configurations	R	1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, G, 17 (operator's own password)
User	Security Configuration Management	RW	1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, G, 17 (operator's own password)
User, CO	Show Status	R	1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, G,
S-S VPN	VPN	R	10, 11, 12, 13, B, C, H
RA VPN	VPN	R	1, 2, 3, 4, 5, 6, 14, 15, 17, A, B, C, D
CO	Software Update	RW	1, 2, 3, 4, 5, 6, 7, 8, 9, 16, A, B, C, D, E, F, G
Unauthenticated	Self-Tests	W	J
Unauthenticated	Show Status	N/A	N/A

Role	Authorized Service	Mode	Cryptographic Key or CSP
Unauthenticated	Zeroize	Z	All CSPs are zeroized.

6 Physical Security Policy

There are no applicable FIPS 140-2 physical security requirements.

7 Operational Environment

The hypervisor environment provides isolated operating environment and is the single operator of the virtual machine. The module was tested on the following environments operating on a general-purpose computing platform.

1. VMware ESXi v5.5 running on a Dell PowerEdge R730
2. VMware ESXi v5.5 running on a PacStar 451
3. KVM on CentOS 7.2 running on a Dell Power Edge R730
4. Microsoft HyperV 2012R2 running on Dell PowerEdge R730
5. Amazon AWS M4.Xlarge EC2 instance*
6. Microsoft Azure Standard D4 v2*

The tested operating environments isolate virtual systems into separate isolated process spaces. Each process space is logically separated from all other processes by the operating environments software and hardware. The module functions entirely within the process space of the isolated system as managed by the single operational environment. This implicitly meets the FIPS 140-2 requirement that only one entity at a time can use the cryptographic module.

*Note: These operational environments are Vendor Affirmed. See Section 8 for operator porting rules.

8 Security Rules

The module design corresponds to the module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 module.

1. The cryptographic module provides four distinct operator roles. These are the User role, Remote Access VPN role, Site-to-site VPN role, and the Cryptographic Officer role.
2. The cryptographic module provides identity-based authentication.
3. The cryptographic module clears previous authentications on power cycle.

4. When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
5. The module supports the generation of key material with the approved DRBG. The entropy provided must be equal to or greater than the security strength of the key being generated. The approved DRBG requests a minimum of 256 bits of entropy per every 384 bits of seed input.

6. The cryptographic module performs the following tests
    A. Power up Self-Tests
        1. Cryptographic algorithm tests
            a. AES Encrypt Known Answer Test
            b. AES Decrypt Known Answer Test
            c. AES GCM Encrypt Known Answer Test
            d. AES GCM Decrypt Known Answer Test
            e. AES CCM Encrypt Known Answer Test
            f. AES CCM Decrypt Known Answer Test
            g. RSA Sign Known Answer Test
            h. RSA Verify Known Answer Test
            i. RSA Encrypt Known Answer Test
            j. RSA Decrypt Known Answer Test
            k. ECDSA Sign Known Answer Test
            l. ECDSA Verify Known Answer Test
            m. HMAC-SHA-1 Known Answer Test
            n. HMAC-SHA-256 Known Answer Test
            o. HMAC-SHA-384 Known Answer Test
            p. HMAC-SHA-512 Known Answer Test
            q. SHA-1 Known Answer Test
            r. SHA-256 Known Answer Test
            s. SHA-384 Known Answer Test
            t. SHA-512 Known Answer Test
            u. DRBG SP800-90A Known Answer Tests
            v. SP 800-90A Section 11.3 Health Tests
            w. DH Known Answer Test
            x. ECDH Known Answer Test Per IG 9.6
    B. Software Integrity Test –verified with HMAC-SHA-256 and ECDSA P-256.
    C. Critical Functions Tests

        1. N/A

    D. Conditional Self-Tests

        1. Continuous Random Number Generator (RNG) test – performed on NDRNG and DRBG
        2. RSA Pairwise Consistency Test (when a key generation fails, the error message displayed is "Cannot verify key and certificate.")
        3. ECDSA Pairwise Consistency Test (when a key generation fails, the error message displayed is "Cannot verify key and certificate.")
        4. Software Load Test – Verify RSA 2048 with SHA-256 signature on software at time of load
        5. If any conditional test fails, the module will output description of the error.

7. The operator can command the module to perform the power-up self-test by cycling power of the module.
8. Power-up self-tests do not require any operator action.
9. Data output is inhibited during power-up self-tests, zeroization, and error states.
10. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
11. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
12. The module does not support a maintenance interface or role.
13. The module does not have any external input/output devices used for entry/output of data.
14. The module does not enter or output plaintext CSPs.
15. The module does not output intermediate key generation values.

Vendor imposed security rules:

1. If the cryptographic module remains inactive in any valid role for the administrator specified time interval, the module automatically logs out the operator.
2. When configured, the module enforces a timed access protection mechanism that supports at most ten authentication attempts per minute. After the administrator specified number of consecutive unsuccessful password validation attempts have occurred, the cryptographic module shall enforce a wait period of at least 1 minute before any more login attempts can be attempted. This wait period shall be enforced even if the module power is momentarily removed.

Operator porting rules:

The CMVP allows user porting of a validated software module to an operational environment which was not included as part of the validation testing. An operator may install and run a VM-series firewall on any general purpose computer (GPC) or platform using the specified hypervisor and operating system on the validation certificate or other compatible operating and/or hypervisor system and affirm the modules continued FIPS 140-2 validation compliance.

The CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when ported and executed in an operational environment not listed on the validation certificate.

Reference: FIPS 140-2 Implementation Guidance G.5

9 Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks outside of the scope of FIPS 140-2, so these requirements are not applicable.

10 References

[FIPS 140-2] FIPS Publication 140-2 Security Requirements for Cryptographic Modules

11 Definitions and Acronyms

AES – Advanced Encryption Standard

CA – Certificate authority

CBC – Cipher Block Chaining

CC – Common Criteria

CCM – Counter with CBC MAC

CO – Cryptographic Officer

CSP – Critical Security Parameter

DHE – Diffie-Hellman Ephemeral

DRBG – Deterministic Random bit generator

ECDHE – Elliptic Curve Diffie-Hellman Ephemeral

ECDSA – Elliptic Curve Digital Signature Algorithm

FIPS – Federal Information Processing Standard

GCM – Galois Counter Mode

HMAC – Hashed Message authentication

IKE – Internet Key Exchange

IP – Internet Protocol

IPSec – Internet Protocol Security

CPU – Central Processing Unit

RAM – Random Access Memory

HDD – Hard Disk Drive

LED – Light Emitting Diode

MAC – Message Authentication Code

NDRNG – Non-deterministic Random Number Generator

OVF – Open Virtualization Format

PAN-OS – Palo Alto Networks' Operating System

RA VPN – Remote Access Virtual Private Network

SNMP – Simple Network Management Protocol

S-S VPN – Site to site Virtual Private Network

SSH – Secure Shell

SSL – Secure Sockets Layer

TLS – Transport Layer Security

VM – Virtual Machine

VPN – Virtual Private Network